James E. Cecchi, Esq.
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Telephone: (973) 994-1700
Email: jcecchi@carellabyrne.com

Attorney for Plaintiff and the putative Class

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

L.C., *A Minor, By And Through Their Legal Guardian* VIVIAN CABRERA, *Individually And On Behalf Of All Others Similarly Situated*, Plaintiff, vs. POWERSCHOOL HOLDINGS, INC. and BAIN CAPITAL, LP, Defendants.	Civil Action No. _____ **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

TABLE OF CONTENTS

CLASS ACTION COMPLAINT

Plaintiff L.C. ("Plaintiff"), a minor, by and through her legal guardian, Vivian Cabrera, on behalf of herself and all others similarly situated, brings this class action against PowerSchool Holdings, Inc. ("PowerSchool") and Bain Capital, LP ("Bain Capital," together "Defendants") to obtain damages, restitution, and/or injunctive relief for herself and on behalf of the proposed Class as defined herein. Plaintiff makes the following allegations upon information and belief, the investigation of her counsel, and facts that are of public record, except as to his allegations, which are made with personal knowledge.

INTRODUCTION

1. This action arises from Defendants' failure to secure personal identifiable information ("PII," referred to herein as "Private Information")[1] of Plaintiff and the members of the proposed Classes, including their names, email addresses, phone numbers, social security numbers, medical information (*e.g.*, food allergies and learning disabilities), dates of birth, reduced meal statuses (*i.e.*, financial information), demographic information, and student and staff identification numbers.

2. PowerSchool is one of the nation's leading providers of cloud-based education software for school administrators. Headquartered in Folsom, California, PowerSchool has an estimated 18,000 customers worldwide, including schools and school districts ranging from kindergarten to twelfth grade levels. In providing its services, PowerSchool created, collected, and maintained the Private Information for Class Members (defined below).

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, but not limited to, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

3. On or about January 9, 2025, PowerSchool publicly announced that it experienced a breach of its national student information system ("SIS") as a result of a vulnerability (the "Data Breach"). Specifically, one or more unauthorized parties were able to gain access to PowerSchool's systems and data by accessing and using compromised credentials.

4. PowerSchool failed to discover its network vulnerability and the unauthorized access to its systems until December 28, 2024. Developing evidence suggests these parties may have gained access to PowerSchool's even earlier.

5. Preliminary reports indicate that PowerSchool failed to implement and/or improperly configured a multi-factor authentication ("MFA") protocol to ensure effective authentication and access security. At a minimum, MFA—widely recognized as a necessary best practice—could have flagged or prevented unauthorized third party access through compromised credentials.

6. PowerSchool was obligated—by contract, industry standards, common law, and its representations to its customers, including Plaintiff and other Class Members—to secure their Private Information from unauthorized disclosures. Plaintiff and Class Members entrusted their Private Information to PowerSchool with the understanding that PowerSchool and any business partners to whom PowerSchool may disclose the Private Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

7. Notwithstanding its obligations, it is apparent from the reported nature and extent of the Data Breach, and Defendants' response thereto, that Defendants failed to take reasonable, timely and appropriate measures to protect against the foreseeable unauthorized disclosure of Private Information.

8. As a direct and proximate result of Defendants' failures, Plaintiff and Class Members have suffered and will indefinitely suffer serious injury.

9. Accordingly, Plaintiff, on behalf of herself and the estimated millions of similarly situated victims of the Data Breach, seeks to hold Defendants responsible for the injuries suffered as the result of their misconduct and failure to act, and demands appropriate monetary, equitable, injunctive, and declaratory relief.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 putative members in the proposed class, and at least one Class Member (*e.g.*, Plaintiff) is a citizen of a state different from Defendants.

11. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged are part of the same case or controversy.

12. This Court has personal jurisdiction over Defendants because Defendants purposefully availed themselves in this District. PowerSchool contracted with West New York School District in New Jersey and agreed to securely store Plaintiff's data. Likewise, Bain Capital, upon the acquisition of PowerSchool in 2024, inherited PowerSchool's assets and liabilities. Plaintiff's claims arise out of or relate to Defendants' purposeful availment in New Jersey. Had Defendants not contracted with, communicated, and availed itself in New Jersey, Plaintiff would not have had their data disclosed in the Data Breach. Accordingly, the exercise of personal jurisdiction here comports with traditional notions of fair play and substantial justice.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District, Plaintiff resides in this District, and Defendants do business in this District.

PARTIES

14. Plaintiff L.C., a minor, by and through their legal guardian Vivian Cabrera ("Plaintiff"), is a resident and citizen of the State of New Jersey and a student of West New York School District, an institution that relied on Defendants to manage the Personal Information of its students and teachers. Plaintiff used Defendants products for education services, and provided highly sensitive Personal Information to Defendants in order to receive education services. Plaintiff provided highly sensitive Personal Information based on the reasonable assumption that Defendants would secure and safeguard Personal Information with adequate security and privacy measures and protect Personal Information from unauthorized disclosure and as a condition of receiving education services. Further, Plaintiff provided Personal Information based on the reasonable assumption that Defendants would provide prompt and timely notification of any unauthorized disclosure of Personal Information to mitigate, among other things, the risks of identity theft and fraud. As a result of Defendants' misconduct, which caused the Data Breach, Plaintiff has, and will have to, take measures that would not otherwise be necessary to protect against identity theft and/or credit disruptions. On March 7, 2025, Plaintiff learned of the Data Breach through a weekly news letter sent to parents of middle school students by West New York School District, the newsletter referenced a notice that is attached hereto as **Exhibit A**. Plaintiff was therefore notified for the first time when receiving the March 7th newsletter that her that her Private Information had been accessed and removed without her authorization. As a result, Plaintiff has begun credit monitoring.

15. PowerSchool Holdings, Inc. ("PowerSchool") is a Delaware company founded in 1997 and is headquartered at 150 Parkshore Drive, Folsom, CA 95630. Defendants offers a wide range of products and services including: a Student Information System platform; document management system; enrollment/attendance manager; recruitment platform; parent communication platform; and Naviance, a tool for planning a student's academic success, to clients in the education industry.

16. Bain Capital, LP ("Bain Capital") is a Delaware company headquartered in Boston, Massachusetts. Bain Capital is a multi-asset investment firm with asset classes including private equity, credit, public equity, venture capital, real estate, life sciences, insurance and other areas of focus. The firm has more than 1,750 employees and approximately $185 billion in assets under management. In 2024, PowerSchool was acquired by Bain Capital. Prior to Bain Capital's acquisition, PowerSchool was accused of improperly managing and selling student data in class action lawsuit filed in California. *See Cherkin v PowerSchool Holdings, Inc.*, No. 3:24-cv-02706 (N.D. Cal.). Julie Liddell, who represents plaintiff Cherkin in this lawsuit, stated that PowerSchool and similar are companies are "data brokers — they're called identity-resolution companies — that collect information from internet users, re-identify the data, and then sell it," and that following Bain Capital's acquisition, PowerSchool "will no longer be legally bound to make even the minimum disclosures required by a public company[.]"[2]

[2] Laura Italiano, *A lawsuit accuses Bain Capital's PowerSchool of trafficking in student data. The edtech giant says everything it does is legal*, INSIDER https://www.yahoo.com/news/lawsuit-accuses-bain-capitals-powerschool-102801213.html (last accessed: Mar. 21, 2025).

REGULATORY FRAMEWORK AND STANDARDS GOVERNING CREATION, COLLECTION, MAINTENANCE, AND USE OF PRIVATE INFORMATION

17. Federal and state regulators have established security standards and issued guidelines and recommendations to reduce the risk of cyberattacks, data breaches, and the resulting consumer harm. There are a number of state and federal laws, requirements, and industry standards governing the creation, collection, protection, and use of Private Information.

18. PowerSchool knew or should have known of the obligations, standards, guidelines, and recommendations with respect to their creation, collection, maintenance, protection, and use of Private Information.

A. The Federal Trade Commission Act (FTCA)

19. The Federal Trade Commission ("FTC") "works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers." The Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair or deceptive acts or practices in or affecting commerce."

20. The FTC has determined that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.

21. Consequently, the FTC has issued numerous guidelines to identify best data security practices that businesses, such as Defendant, should employ to protect against unlawful exposure of Private Information.

22. The FTC's guidance for businesses underscores the importance of implementing and maintaining reasonable data security practices.[3] For example, the FTC offers the following general guidelines:

- In managing confidential information, businesses should factor security into the decision making in every department of the business—personnel, sales, accounting, information technology, etc.
- Don't collect personal information you don't need, and hold on to information only as long as you have a legitimate business need.
- Don't use personal information when it's not necessary.
- Use an intrusion detection system to expose a breach as soon as it occurs.
- Watch for large amounts of data being transmitted from the system.
- Have a response plan in the event of a breach.

23. With respect to updates and patches to third-party software, the FTC states that outdated software undermines security, the solution being to update software regularly, implement third-party patches as they are issued, prioritize patches by the severity of the threat they are designed to avert, and use automated tools to track which version of software is running and whether updates are available.

24. Consequently, the FTC strongly encourages businesses to "[p]ut procedures in place to keep your security current and address vulnerabilities that may arise," including to "[c]heck expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches

[3] *Start with Security: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/start-security-guide-business#start (last visited March 17, 2025).

to correct problems."[4] The FTC's website cites an example case, wherein it charged that a business failed to patch a critical vulnerability because its patch management policies and procedures were inadequate.

25. With respect to security warnings in regard to vulnerabilities, the FTC cautions businesses to heed credible security warnings and move quickly to fix them. The FTC also strongly encourages businesses to "[h]ave an effective process in place to receive and address security vulnerability reports." Citing an example case, wherein the FTC charged that a business' alleged delay in responding to warnings meant that the vulnerabilities found their way onto additional devices and across multiple system versions, the FTC warns: "When vulnerabilities come to your attention, listen carefully and then get a move on."

26. The FTC has routinely brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice prohibited by the FTCA. Orders derived from these enforcement actions explicate the measures businesses must take to satisfy obligations concerning data security.

B. State Laws Concerning Private Information

27. At least 24 states have enacted laws addressing data security practices, requiring businesses that own, license, or maintain Private Information about a resident to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

28. Among other requirements, § 521.052 imposes certain requirements on businesses with respect to the protection of sensitive personal information including, but not limited to, that

[4] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited March 17, 2025).

the "business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business" and "shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by (1) shredding; (2) erasing; or (3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means."

29. Additionally, § 521.053 requires notification by the business to impacted individuals in the event of a breach of system security, including that the business "shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

30. Pursuant to § 521.05, notification to the impacted individual "shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred."

C. Industry Standards

31. Various cybersecurity industry best practices have been published, are readily available, and should be consulted as a go-to source for an entity instituting, developing, maintaining, or enhancing its cybersecurity standards.

32. These practices include, across all industries encountering Private Information, education and appropriate access restriction for all personnel in regard to proper creation, collection, maintenance, and use of Protected Information; enforcing strong password and similar protections, including multi-factor authentication; applying multi-layer security measures (including firewalls, antivirus, and anti-malware software); monitoring for suspicious or irregular

traffic to servers, credentials used to access servers, activity by known or unknown users, and server requests; implementing encryption to render data unreadable without proper authorization; and regular back up of data.

33. Additional cybersecurity best practices include, but are not limited to, installing appropriate malware detection software, monitoring and limiting network posts, securing web browsers and e-mail systems, configuring network infrastructure (like firewalls, switches, and routers), safeguarding physical security systems, training staff on key cybersecurity aspects, monitoring for vulnerability alerts, and promptly detecting and addressing vulnerability alerts before exploitation by cybercriminals.

34. In addition to commonly recognized industry best practices, the National Institute of Standards and Technology ("NIST") and the Center for Internet Security, Inc. ("CIS")[5] have established standards for reasonable cybersecurity readiness.

35. Recognizing that the national and economic security of the United States is dependent upon the reliable function of critical infrastructure, President Barrack Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. Executive Order 13636 directed NIST to work with stakeholders to develop a voluntary

[5] CIS is a community-driven nonprofit responsible for globally recognized best practices for securing IT systems and data, including a prescriptive, prioritized, and simplified set of best practices in cybersecurity (referred to as "CIS Controls") and consensus-based prescriptive configuration recommendations of global cybersecurity experts (referred to as "CIS Benchmarks"). Per the CI website, the CIS Controls are a general set of recommended practices for securing a wide range of systems and devices, whereas CIS Benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices. The need for secure configurations is referenced throughout the CIS Controls. In fact, CIS Control 4 specifically recommends secure configurations for hardware and software on mobile devices, laptops, workstations, and servers. Both the CIS Controls and the CIS Benchmarks are developed by communities of experts using a consensus-based approach. *See* https://www.cisecurity.org/controls/cis-controls-faq (last visited March 17, 2025).

framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. Created through collaboration between industry and government, the voluntary framework promotes the protection of critical infrastructure, and provides standards, guidelines, tools, and technologies to protect information technology systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services.

36. For example, NISTIR 8374, a NIST publication titled "Ransomware Risk Management: A Cybersecurity Framework Profile," provides the following essential ransomware tips:

- Educate employees on avoiding ransomware infections.
    - Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.
    - Avoid using personal websites and personal apps—like e-mail, chat, and social media—from work computers.
    - Don't connect personally owned devices to work networks without prior authorization.
- Avoid having vulnerabilities in systems that ransomware could exploit.
    - Keep relevant systems fully patched. Run scheduled checks to identify available patches to install these as soon as feasible.
    - Employ zero trust principles in all networked systems. Manage access to all network functions and segment internal networks where practical to prevent malware from proliferating among potential target systems.

- Allow installation and execution of authorized apps only. Configure operating systems and/or third party software to run only authorized applications.
- Inform your technology vendors of your expectations (*e.g.*, in contract language) that they will apply measures that discourage ransomware attacks.

- Quickly detect and stop ransomware attacks and infections.
  - Use malware detection software such as antivirus software at all times. Set it to automatically scan e-mails and flash drives.
  - Continuously monitor directory services (and other primary user stores) for indicators of compromise or active attack.
  - Block access to untrusted web resources. Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity.
- Make it harder for ransomware to spread.
  - Use standard user accounts with multi-factor authentication versus accounts with administrative privileges whenever possible.
  - Introduce authentication delays or configure automatic account lockout as a defense against automated attempts to guess passwords.
  - Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has only the necessary access following the principle of least privilege.

- Store data in an immutable format (so that the database does not automatically overwrite older data when new data is made available).
- Allow external access to internal network resources via secure virtual private network (VPN) connections only.

- Make it easier to recover stored information from a future ransomware event.
  - Make an incident recovery plan. Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization and business continuity plans for those critical services.
  - Back up data, secure backups, and test restoration. Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
  - Keep your contacts. Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

FACTUAL ALLEGATIONS

A. PowerSchool's Business

37. Defendants are the largest provider of cloud-based education software for K-12 education in the United States, with 18,000 customers across North America, making it responsible for the Personal Information of over fifty (50) million students, teachers, and their family members in the country. PowerSchool retains historical information of former students and teachers who previously made use of its systems, dating back to 2005.

38. PowerSchool services its customers in more than ninety (90) countries including throughout North America—specifically, private and public schools and school districts. PowerSchool offers its school-customers a variety of products aimed at managing educational administrative tasks like enrollment, attendance, parent notifications, emergency contacts, assignments, grades, transcripts, student medical records, and staff recruitment.

39. PowerSchool also offers a variety of cloud-software products for schools to customize to meet their needs and accomplish administrative tasks. One of PowerSchool's leading products is the PowerSchool SIS, used by at least 15,000 schools and districts across the country

40. As part of its services, PowerSchool collects and retains a wide variety of highly sensitive Personal Information, including:[6]

- Name;
- Email Address;
- Social Security Number;
- Address;
- Phone Number;
- Emergency Contact Information;
- Birth Date;
- Age;
- Grade;
- Gender;
- Device Information (e.g. unique device ID, IP address, and cookies);

[6] PowerSchool*'s Privacy Principles*, PowerSchool, https://www.PowerSchool.com/privacy/ (last visited March 17, 2025).

- Class Schedule;
- Standardized Test Scores;
- Grades;
- Allergy Information;
- Immunization Records; and
- Learning Disabilities.

41. In short, this Personal Information is highly sensitive and can be exploited by unauthorized parties to engage in fraudulent activities such as identity theft and other forms of fraud.

B. The Data Breach

42. On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of certain personal information from PowerSchool Student Information System (SIS) environments through one of our community-focused customer support portals, PowerSource.[7]

43. For involved individuals, the types of information exfiltrated in the incident included one or more of the following, which varied by person: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number, and other related information.[8]

[7] *Notice of Data Breach for Individuals in the United States*, PowerSchool, https://www.PowerSchool.com/security/sis-incident/notice-of-united-states-data-breach/ (last visited March 17, 2025).
[8] *Id.*

44. A March 2025 CrowdStrike forensic report confirmed the breach was caused by a compromised credential, but the root cause of how the compromised credential was acquired and used remains unknown.[9]

45. Mark Racine, chief executive of the Boston-based education technology consulting firm RootED Solutions, told TechCrunch that while the report provides "some detail," there is not enough information to "understand what went wrong."[10]

46. As a result of the Data Breach, PowerSchool stated that it is offering two years of complimentary identity protection services to students and educators whose information was involved. For adult students and educators, this offer will also include two years of complimentary credit monitoring services.

47. On or about January 9, 2025, PowerSchool publicly announced the Data Breach and began sending notifications to impacted parties, such as to Plaintiff and Class Members, to advise of the Data Breach.

C. Defendants Failed to Comply with Regulatory Requirements and Standards, and Breached Contracts with and Duties Owed to Plaintiff and Class Members

48. On information and belief, PowerSchool failed to comply with the FTCA. On information and belief, Defendants failed to: heed credible security warnings; failed to maintain adequate patch management policies and procedures; failed to detect alerts regarding vulnerabilities affecting its systems; failed to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failed to properly use automated tools to track which versions of software

[9] Carly Page, *What* PowerSchool *won't say about its data breach affecting millions of students*, TechCrunch, https://techcrunch.com/2025/03/10/what-PowerSchool-isnt-saying-about-its-massive-student-data-breach/ (last visited March 17, 2025).
[10] *Id.*

were running and whether updates were available; failed to implement appropriate procedures to keep security current and address vulnerabilities, including failure to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities; and failed to encrypt or otherwise adequately protect Plaintiff's and Class Members' Private Information.

49. On information and belief, Defendants' failure to protect and safeguard the Private Information of Plaintiff and Class Members resulted in the disclosure of such information to one or more third-parties without consent, in violation of FTCA. Such disclosure was not necessary to carry out the purpose for which Defendants received the information, nor was it permitted by statute, regulation, or order.

50. Defendants' violations of FTCA, as set forth above, were reckless or, at the very least, negligent.

51. On information and belief, Defendants also failed to implement and comply with cybersecurity industry standards. Defendants failed to meet the minimum standards of any of the following best practices and frameworks: CIS and NIST publications (including, without limitation, "Ransomware Risk Management: A Cybersecurity Framework Profile"), the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and CIS's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness and response.

D. The Private Information Accessed in the Date Breach is Highly Valuable

52. The Private Information of consumers is a valuable commodity and, consequently, a frequent intentional target of cybercriminals.

53. The value of Private Information is axiomatic, considering the value of "big data" in corporate America and the fact the consequences of cybercrimes include heavy criminal

penalties. The risk-to-reward analysis illustrates that Private Information has considerable market value.

54. Indeed, the U.S. Attorney General confirmed in 2020 that "hackers" target consumers' sensitive personal information because it "has economic value."[11]

55. Numerous sources cite "dark web" pricing for stolen Private Information.[12]

56. According to various sources, Private Information can be sold at prices ranging from $40.00 to $200.00 per record, bank details can be sold at prices ranging from $50.00 to $200.00 per record,[13] and a stolen credit or debit card number can sell for $5.00 to $110.00.[14]

[11] *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (February 10, 2020), available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited March 17, 2025).

[12] In pertinent part, Wikipedia defines the "dark web" as:

> World Wide Web content that exists on darknets: overlay networks that use the internet but require specific software, configurations, or authorizations to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (October 16, 2019), *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-darkweb-how-much-it-costs/ (last visited March 17, 2025).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (December 6, 2017), *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-yourpersonal-information-is- selling-for-on-the-dark-web/ (last visited Jan. 31, 2024).

57. In addition, criminals can purchase access to the entirety of a company's breached database on the dark web,[15] and would expect a sale price of $999.00 to $4,995.00.[16]

58. Relatively basic information such as names, e-mail addresses, and phone numbers, have value to cybercriminals. In addition to practices such as "spamming" customers or launching "phishing" attacks using compromised names and e-mails, cybercriminals routinely combine this information with other compromised data to build a more complete profile of an individual. As reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing e-mails," it is often such consumer profiling that enables cybercriminals to successfully carry out additional phishing attacks or social engineering attacks.[17]

59. There is often a substantial time lag between when a harm occurs as the result of a breach and when the harm is discovered, as well as substantial lag time between when Private Information is compromised and when it is used. According to the U.S. Government Accountability Office,[18] which performed a comprehensive analysis of data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold

---

[15] *See, e.g., In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymousbrowsing/in-the- dark/ (last visited March 17, 2025); *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.16, 2019, *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-darkweb-how-much-it-costs/ (last visited March 17, 2025).

[16] *In the Dark*, VPNOverview (2019), *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited March 17, 2025).

[17] *See Dark Web Price Index: The Cost of Email Data*, available at https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited March 17, 2025).

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. Government Accountability Office (June 4, 2007), available at: https://www.gao.gov/products/gao-07-737 (last visited March 17, 2025).

or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

60. In any event, once cybercriminals compromise Private Information, they often trade the information on the "cyber black market" for many years.

E. The Data Breach was a Foreseeable Risk

61. It is well known that entities involved in the routine creation, collection, maintenance, and use of Private Information, are at a heightened risk of a cyberattack.

62. At all relevant times, PowerSchool's susceptibility to a cyberattack was or reasonably should have been known and obvious to Defendant.

63. At all relevant times, PowerSchool was or should have been aware of the significant number of individuals whose Private Information PowerSchool created, collected, and stored and, thus, the significant number of individuals who would be harmed by unauthorized access to its systems.

64. At all relevant times, PowerSchool was or should have been aware that the Private Information of Plaintiff and Class Members was an attractive target for malicious actors.

65. At all relevant times, PowerSchool knew or reasonably should have known of the importance of safeguarding Private Information and the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

66. PowerSchool's failure to safeguard Private Information is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data. Indeed, data breaches, such as the one experienced by PowerSchool have become so notorious that the FBI, U.S. Secret

Service, and other authorities have issued warnings to potential targets so they are aware of, can prepare for and, hopefully, are able to ward off a potential attack.

67. As early as 2011, the FBI issued warnings regarding the advancement in cybercriminals' ability to attack systems remotely and exploit them to obtain Private Information. This warning was not only a prediction of the general escalation of cybercrime, but also a clear indication to entities such as PowerSchool of the impending risks associated with storing and handling sensitive data.[19]

68. In addition, trends in cybercrime have demonstrated an alarming increase in the frequency and sophistication of attacks. These attacks include, without limitation, attacks on the following entities: Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020). Thus, PowerSchool knew or should have known that cybercriminals would target the Private Information that it collected and maintained.

69. The continual increase in data breaches underscored the necessity for PowerSchool to implement advanced security measures, such as robust encryption, regular security audits, and comprehensive employee training on cybersecurity.

70. Based on the foregoing, PowerSchool knew or should have known that its data systems would be targeted by cybercriminals and had an obligation and duty to take all reasonable means to protect Private Information from attacks such as the Data Breach here.

[19] Gordon M. Snow, *Statement before the House Financial Service Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cybersecurity-threats-to-the-financial-sector (last visited March 17, 2025).

71. Notwithstanding the common knowledge of, and the prevalence of public announcements and abundance of other publicly available resources with respect to, the imminent and serious threat of unauthorized access to Private Information, and despite its creation, collection, maintenance, and use of Private Information of millions of individuals, Defendants failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' Private Information. Had Defendants implemented adequate security measures, cybercriminals never could have accessed Private Information for millions of Defendants' customers and the Data Breach would have been prevented or, at a minimum, of a much smaller scope.

F. The Data Breach Harmed and Will Continue to Harm the Class

72. Victims of data breaches are exposed to serious ramifications. Indeed, the reason why cybercriminals steal sensitive information is to monetize it.

73. Cybercriminals monetize stolen personal identification, health, and financial information by selling, on the black market, the spoils of their cyberattacks to identity thieves and other criminals to extort and harass victims or assume the victims' identities to engage in illegal financial transactions under the victims' names.

74. Victims of identity theft also routinely suffer embarrassment, harassment, or blackmail, in person or online, and/or experience financial losses (*e.g.*, unauthorized account transactions and credit downgrades) resulting from, by way of example, fraudulently opened accounts or misuse of existing accounts.

75. The unencrypted Private Information of Plaintiff and Class members will end up (to the extent that it has not already ended up) for sale on the dark web, as that is the modus operandi of cybercriminals.

76. Given the type and scope of this targeted attack, the sophisticated cybercriminal activity, the volume of data compromised, and the sensitive type of Private Information involved in this Data Breach, entire batches of stolen information have undoubtedly been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes, including opening financial and other accounts in the consumer's name to make purchases or to launder money; filing of fraudulent tax returns; taking of loans or lines of credit; or filing of false unemployment or similar claims.

77. Unencrypted Private Information may also fall into the hands of other entities that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

78. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn the circumstances of the breach, and attempt to mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking such steps—including failure to constantly review accounts and credit reports—could expose the individual to greater financial harm.

79. Thus, due to the imminent risk of or completed identity theft, Plaintiff and Class Members must monitor their financial accounts for many years in an attempt to mitigate the risk of identity theft, and now face years of constant surveillance of their financial and personal records, other necessary monitoring, and loss of rights.

80. The retail cost of credit or identity theft monitoring is expected to be approximately $200 per year per Class Member. This is a reasonable and necessary cost to monitor and protect Plaintiff and Class Members from the risk of identity theft resulting from Defendants' Data Breach.

This is a future cost for, at a minimum, five years. Plaintiff and Class Members would not be caused to bear this expense but for Defendants' failure to safeguard their Private Information.

81. Plaintiff and Class members have spent and will continue to spend, time on various prudent actions, such as changing passwords and re-securing their own computer systems.

82. Defendants' failure to properly safeguard Plaintiff's and Class Members' Private Information from cybercriminals has caused and will continue to cause substantial risk of future harm (such as identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off such highly sensitive information.

CLASS ALLEGATIONS

83. Plaintiff brings this class action individually on behalf of herself and on behalf of all members of the following classes and subclasses (collectively, the "Classes") of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23(a) and 23(b)(3) (as well as the requirements for certification of one or more issue classes under Rule 23(c)(4)).

84. Accordingly, Plaintiff seeks certification under Federal Rule of Civil Procedure 23 of the following Classes and Subclasses:

STUDENT CLASS

Nationwide Class: All individual students residing in the United States whose Private Information was exposed, accessed, and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

New Jersey Subclass: All individual students residing in the State of New Jersey whose Private Information was exposed, accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

TEACHER CLASS

Nationwide Class: All individual teachers residing in the United States whose Private Information was exposed, accessed, and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

New Jersey Subclass: All individual teachers residing in the State of New Jersey whose Private Information was exposed, accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

85. Excluded from the Classes are (1) Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, any entity in which Defendants has a controlling interest; (2) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (3) those persons who have suffered personal injuries as a result of the facts alleged herein (4) any and all federal, state, or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions; and (5) all judges presiding over this matter or assigned to hear any aspect of this litigation, along with judicial clerks and staff, and immediate family members.

86. Plaintiff reserves the right to modify or amend the foregoing Class and Subclass definitions before the Court determines whether certification is appropriate.

87. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is readily ascertainable.

88. **Numerosity (Federal Rule of Civil Procedure 23(a)(1)):** A class action is the only available method for the fair and efficient adjudication of this controversy. The members of each Class are so numerous and geographically dispersed that individual joinder of all Class Members is neither practicable nor possible. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the millions of individuals. Membership in the Class will be determined by analysis of Defendants' records.

89. **Commonality (Federal Rule of Civil Procedure 23(a)(2) and (b)(3)):** Consistent with Rule 23(a)(2) and with Rule 23(b)(3)'s predominance requirement, Plaintiff and Class Members share a community of interest in that there are numerous common questions and issues of law and fact which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their Private Information;

b. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

c. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

d. Whether Defendants was negligent in maintaining, protecting, and securing Private Information;

e. Whether Defendants was negligent in failing to adequately monitor and audit the data security systems;

f. Whether Defendants breached its duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the data breach was discovered;

h. Whether Defendants failed to take reasonable and prudent security measures;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants' security measures to protect its systems were reasonable in light of known legal requirements;

k. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

l. Whether Defendants violated state consumer protection and state information privacy laws in connection with the actions described herein;

m. Whether Defendants violated federal statutes including, but not limited to, FTCA;

n. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

o. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

p. Which security procedures and notification procedures Defendants should be required to implement;

q. Whether Defendants was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

r. Whether Defendants' conduct, including its alleged failure to act, resulted in or was the proximate cause of the Data Breach and/or loss of Private Information of Plaintiff and Class Members;

s. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Private Information; and

t. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

90. In the alternative, Plaintiff seeks certification under Rule 23(c)(4) with respect to one or more of the above issues or such other issues as may be identified in the future.

91. **Typicality (Federal Rule of Civil Procedure 23(a)(3)):** Plaintiff's claims are typical of the claims of the Classes. Plaintiff's and Class Members' Private Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff sustained damages, akin to damages sustained by Class Members, arising out of and caused by Defendants' common course of conduct in violation of laws and standards, as alleged herein.

92. **Adequacy (Federal Rule of Civil Procedure 23(a)(4)):** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of each of the Classes because Plaintiff is a member of the Classes and is committed to pursuing this matter against Defendants to obtain relief for the Classes. Plaintiff is not subject to any individual defense unique from those conceivably applicable to other Class Members or the Classes in their entirety. Plaintiff anticipates no management difficulties in this litigation. Plaintiff has no conflicts of interest with the Classes. Plaintiff's Counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

93. **Predominance and Superiority (Federal Rule of Civil Procedure 23(b)(3)):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation predominate over individual issues. The issues discussed above in regard to commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action

mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also burden and unreasonably strain the court system, and would result in undue delay. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

94. **Ascertainability:** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. Defendants has access to names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach.

95. **Injunctive and Declaratory Relief:** This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and procedures hinges on Defendants' conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff. Unless a Class-wide injunction is issued, Defendants may continue failing to properly secure Class Members' Private Information, and Defendants may continue to

act unlawfully, as set forth in this Complaint. Further, Defendants has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

CAUSES OF ACTION

COUNT ONE
Negligence
(On Behalf of Plaintiff and the Classes)

96. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

97. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

98. The Private Information of Plaintiff and Class Members was entrusted to Defendants with the understanding that the information would be safeguarded.

99. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

100. It was reasonably foreseeable to Defendants that Plaintiff and the Class Members would suffer such harms in the event of a cyber-attack such as the Data Breach here.

101. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in Defendants' possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

102. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, consistent with industry standards and requirements, and to ensure that its computer

systems, networks, and protocols, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information.

103. Defendants also had a special relationship with Plaintiff and each of the Class Members. That special relationship arose because Defendants was entrusted with their confidential Private Information as a necessary part of the services rendered or goods sold by Defendant. That special relationship provides an additional basis on which Defendants owed a duty to Plaintiff and each of the Class Members to protect against unauthorized access to, theft of, and/or disclosure of their Private Information.

104. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that all Private Information in their possession or control was adequately secured and protected.

105. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in their possession or control, including not sharing information with other entities who maintain sub-standard data security systems.

106. Defendants owed a duty to Plaintiff and Class Members to implement and maintain processes that would immediately detect a breach of their data security systems in a timely manner.

107. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

108. Defendants owed a duty to Plaintiff and Class Members to disclose in timely fashion if their computer systems and data security practices were inadequate in any way to safeguard individuals' Private Information, including from theft, because such an inadequacy would be a material fact in the decision to entrust Private Information to Defendant.

109. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' Private Information.

110. Defendants owed a duty to Plaintiff and Class Members to monitor user behavior and activity to identify possible threats to the confidentiality and integrity of Private Information.

111. Defendants owed a duty to Plaintiff and Class Members to promptly and adequately notify Plaintiff and Class Members of the Data Breach, but failed to do so.

112. Defendants had and continues to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within their possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and remains necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

113. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in creating, collecting, and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on their systems.

114. Plaintiff and the Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

115. Defendants was in a position to protect against the harm suffered by Plaintiff and the Class Members as a result of the Data Breach.

116. Defendants' duties extended to protecting Plaintiff and the Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put

in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

117. Defendants failed to perform its duties by failing to reasonably and adequately secure their systems (and the Private Information of Plaintiff and the Class Members) against the Data Breach.

118. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiff and the Class Members, Plaintiff's and Class Members' Private Information would not have been exposed to the Data Breach and compromised.

119. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class Members.

120. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class Members have suffered and will suffer injury to their privacy, the value of their Private Information, and other forms of injury and/or harm, including, but not limited to, emotional distress, loss of privacy, anxiety, annoyance, nuisance, and other economic and non-economic losses including nominal damages.

121. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

122. Defendants' negligent conduct is ongoing, in that Plaintiff's and Class Members' Private Information is being maintained in an unsafe and insecure manner.

123. Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to: (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual

audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT TWO
Breach of Implied Contract
(On Behalf of Plaintiff and the Classes)

124. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

125. Plaintiff and Class Members were required deliver their Private Information to Defendants as part of the process of obtaining products and/or services from Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for said products and/or services.

126. Defendants solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendant.

127. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or products to Plaintiff and Class Members.

128. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class Members if their data had been breached and compromised or stolen.

129. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

130. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information only for business purposes; (b) take reasonable steps to safeguard the Private Information; (c) prevent unauthorized disclosures of the Private Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

131. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

132. Defendants breached its contractual obligations in regard to the protection of Plaintiff's and Class Members' Private Information, as described in detail herein.

133. Defendants knew that if it were to breach the implied contract with its customers, Plaintiff and Class Members would be harmed.

134. As a direct and proximate result of Defendants' breach of contract, Plaintiff and the Class Members have suffered and/or will suffer injury.

COUNT THREE
Declaratory Judgment
(On Behalf of Plaintiff and the Classes)

135. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

136. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

137. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Defendants' data security measures remain inadequate. In addition, Plaintiff continues to suffer injuries as result of the exposure of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

138. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owes a legal duty to secure Plaintiff's and Class Members' Private Information, select vendors who handle Private Information that will adequately safeguard that information, and to timely and adequately notify impacted individuals of a data breach, and

b. Defendants continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

139. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment awarding Plaintiff and the Classes equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

A. enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein pertaining to the misuse, failure to protect, and/or disclosure of Plaintiff's and Class Members' Private Information;

B. requiring Defendants to implement appropriate security protocols designed to protect the confidentiality and integrity of Private Information, including through:

i. utilization of appropriate methods, procedures, and policies with respect to collection, storage, and use of Private Information;

ii. encryption of all data collected through the course of business in accordance with applicable regulations, industry standards, and federal, state, and local laws;

iii. monitoring of ingress and egress of all network traffic;

iv. engaging independent third-party auditors and internal personnel to run automated security monitoring, simulated attached, penetration tests, and audits on Defendants' systems;

v. segmenting of data by creation of appropriate firewalls and access controls; and

vi. establishing an appropriate and/or supplementing their existing information security training programs;

C. compelling Defendants to issue prompt, complete, specific, and accurate disclosures to Plaintiff and Class Members, with respect to all Private Information compromised as the result of the Data Breach;

D. requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

E. compelling Defendants to facilitate, maintain, and/or pay for credit monitoring services for Plaintiff and the Classes, for a period not less than five years;

F. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

G. appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis, for a period of ten years, to evaluate Defendants' compliance with the terms of the Court's final judgments, to provide such report to the Court and counsel for the Class, and to report any deficiencies with compliance with the Court's judgment.

140. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, Defendant. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

141. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

142. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at or by Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

COUNT FOUR
New Jersey Consumer Fraud Act

N.J.S.A. §§ 56:8-1, et seq.

143. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

144. Defendants are "persons," as defined by N.J.S.A. § 56:8-1(d).

145. Defendants sell "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

146. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2 prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

147. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co*., 138 N.J. 2, 19 (1994).

148. "The standard of conduct that the term 'unconscionable' implies is lack of 'good faith, honesty in fact and observance of fair dealing.'" *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). "In addition, '[i]ntent is not an essential element' for allegations related to unconscionable commercial practices to succeed." *Fenwick v. Kay Am. Jeep, Inc.*, 72 N.J. 372, 379 (1977).

149. Defendants' handling and treatment of Plaintiff's and Subclass Members' Personal Information was unconscionable as described herein.

150. Defendants' handling and treatment of Plaintiffs' and Subclass Members' PII was deceptive because Defendants:

a. Misrepresented that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

b. Misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, et seq.;

c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

d. Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, et seq.

151. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

152. Defendants intended to mislead Plaintiff and Subclass Members and induce them to rely on its omissions of material fact.

153. As a direct and proximate result of Defendants' unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to

monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

154. Plaintiff and Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the proposed Class and Subclass, respectfully request that the Court enter judgment in Plaintiff's favor and against Defendants as follows:

A. Declaring, adjudging, and decreeing that this action is a proper class action, and certifying each of the proposed Classes and/or any appropriate Subclasses pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and/or (b)(3), including designating Plaintiff as Class representative and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class and Subclass appropriate monetary relief, including actual damages; statutory damages; consequential damages; punitive damages; exemplary damages; nominal damages; restitution; and disgorgement of all earnings, interest, profits, compensation, and benefits received as a result of their unlawful acts, omissions, and practices;

C. Awarding Plaintiff and the Classes equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

1. enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein pertaining to the misuse, failure to protect, and/or disclosure of Plaintiff's and Class Members' Private Information;

2. requiring Defendants to implement appropriate security protocols designed to protect the confidentiality and integrity of Private Information, including through:

   a. utilization of appropriate methods, procedures, and policies with respect to collection, storage, and use of Private Information;

   b. encryption of all data collected through the course of business in accordance with applicable regulations, industry standards, and federal, state, and local laws;

   c. monitoring of ingress and egress of all network traffic;

   d. engaging independent third-party auditors and internal personnel to run automated security monitoring, simulated attached, penetration tests, and audits on Defendants' systems;

   e. segmenting of data by creation of appropriate firewalls and access controls; and

   f. establishing an appropriate and/or supplementing its existing information security training program;

3. compelling Defendants to issue prompt, complete, specific, and accurate disclosures to Plaintiff and Class Members, with respect to the Private Information compromised as the result of the Data Breach;

4. requiring Defendants to meaningfully educate Plaintiff and all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

5. compelling Defendants to facilitate, maintain, and/or pay for credit monitoring services for Plaintiff and the Classes, for a period not less than five years;

6. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

7. appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis, for a period of ten years, to evaluate Defendants' compliance with the terms of the Court's final judgments, to provide such report to the Court and counsel for the Class, and to report any deficiencies with compliance with the Court's judgment.

D. Compelling Defendants to pay the costs associated with notification of Class Members about the judgment and administration of claims;

E. Awarding Plaintiff and the Classes pre-judgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Classes reasonable attorneys' fees, costs, and expenses; and

G. Awarding Plaintiff and the Classes such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class and/or Subclass(es), hereby demands a trial by jury of all issues in this Complaint so triable.

Dated: March 21, 2025

Respectfully submitted:

/s/ James E. Cecchi

James E. Cecchi, Esq.
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Telephone: (973) 994-1700
Email: jcecchi@carellabyrne.com

Attorneys for Plaintiff and the putative Class